Block Cipher Chaining Modes of Operation

Lars R. Knudsen
ABTcrypto.com

presented by

Bart Preneel
K.U.Leuven, Belgium and ABTcrypto.com

Accumulated Block Chaining (ABC)

$$\begin{aligned} \text{Encryption:} \quad H_i &= P_i \oplus h(H_{i-1}) \\ C_i &= E_K(H_i \oplus C_{i-1}) \oplus H_{i-1} \end{aligned}$$

$$\begin{aligned} \text{Decryption:} \quad H_i &= D_K(C_i \oplus H_{i-1}) \oplus C_{i-1} \\ P_i &= H_i \oplus h(H_{i-1}) \end{aligned}$$

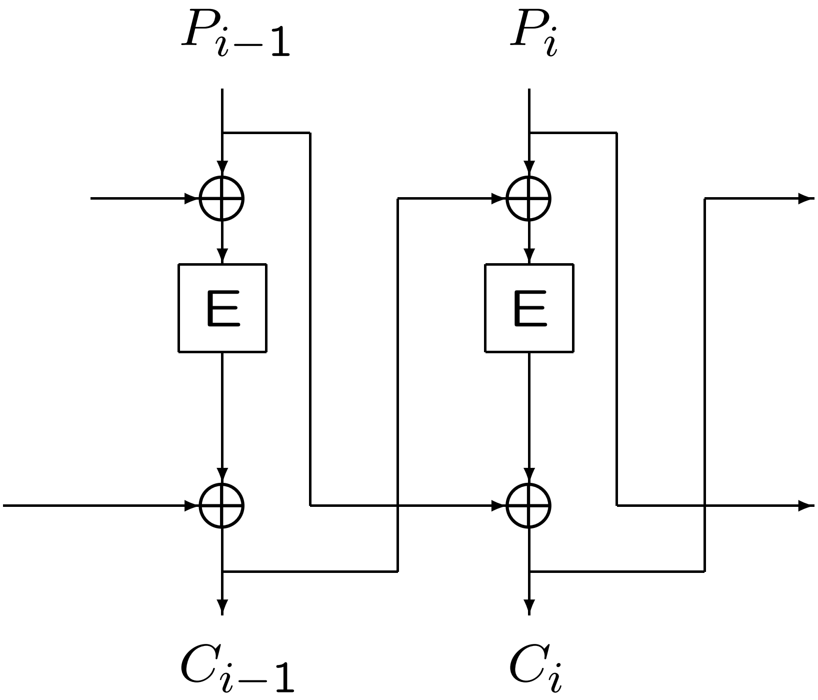
- $h : \{0,1\}^n \rightarrow \{0,1\}^n$,

  $h(X) = X$ **or** $h(X) = X^{<<1}$ seem appropriate

- H_0, C_0 initial values

- ABC with $h(X) = 0$ suggested in 1977 by C. Campbell

Infinite Garble Extension (ABC with $h(X) = 0$)



Accumulated Block Chaining (ABC)

- infinite error propagation

- accumulation of plaintext blocks to avoid low entropy attacks

- birthday attacks not serious

- encryption and decryption operations similar

CBC mode

- $C_i = E_K(P_i \oplus C_{i-1}), \quad P_i = D_K(C_i) \oplus C_{i-1}$

- Error recovery after two blocks

- Birthday attack:

$$\begin{aligned} C_i &= C_j \quad \Rightarrow \\ P_i \oplus C_{i-1} &= P_j \oplus C_{j-1} \quad \Rightarrow \\ P_i \oplus P_j &= C_{i-1} \oplus C_{j-1}. \end{aligned}$$

- Bad diffusion in decryption operation (by nature)

  Man-in-the-middle can fiddle

$$(C_{j-1}, C_j) = (C_{i-1}, C_i) \Rightarrow P_j = P_i$$

ABC mode

- $H_i = P_i \oplus h(H_{i-1})$ $C_i = E_K(H_i \oplus C_{i-1}) \oplus H_{i-1}, \quad H_i = D_K(C_i \oplus H_{i-1}) \oplus C_{i-1}$

- Birthday attack

$$\begin{aligned} H_{i-1} \oplus C_i &= H_{j-1} \oplus C_j \quad \Rightarrow \\ E_K(H_i \oplus C_{i-1}) &= E_K(H_j \oplus C_{j-1}) \quad \Rightarrow \\ H_i \oplus H_j &= C_{i-1} \oplus C_{j-1}. \end{aligned}$$

  If plaintext blocks uniformly distributed condition of match not verifiable

  With $h(X) = X$ or $h(X) = X^{<<1}$ for all practical plaintext spaces flat distribution of H_i (i not tiny)

- Man-in-the-middle cannot fiddle

Error propagation and error recovery

- Many applications for error propagation

- Advantages of modes with error propagation

  - greater resemblance to big sn-bit block cipher
    (s blocks on n bits)

  - resistance against birthday attacks (ciphertext only)

  - better diffusion properties for both encryption and decryption

  - equal operations for encryption and decryption

Message confidentiality and message integrity

- ABC (by itself) does not give message integrity

- Separate issues in our opinion

- Choose good mode for confidentiality, then add
  message integrity if needed

Concluding remarks

- FIPS 81 does not include modes with error propagation
- New standard ought to
- ABC proposed as mode of operation for AES